Sybil Attack Detection through Distance Calculation

A Dissertation Report

Submitted By

Vaishali Aggarwal

To

Department of Computer Science

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Mr. Ravinder Singh
(Assistant Professor)

(May 2015)

PAC approval page

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: Science & Technology

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Vaishali
Registration No: 11301383
Batch: 2K13-2K15
Roll No. A13
Session: 2014-2015
Parent Section: RK2305
Details of Supervisor:
Designation: Asst. Professor
Name Ravinder Singh
Qualification: Mtech
U.ID 17750
Research Experience: 1 yrs

SPECIALIZATION AREA: Networking (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. VANET'S (securing Vanet networks from various live attacks)
2. MANET's
3. Cryptography

Signature of Supervisor 17750

PAC Remarks:
First topic is approved, publication expected.

11/11/15

APPROVAL OF PAC CHAIRPERSON: Signature: Date: 20/9/15

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to Supervisor.

ABSTRACT

VANET is the new upcoming technology that is being increasingly favoured for management of public areas and parking lots, accident avoidance and traffic control. So it is very important to ensure security of VANET. In VANET, many voting based schemes are used for decision making. So, if attacker can easily forge multiple identities then that decision can be easily changed and hence it will affect the normal behavior of VANET. Therefore, an efficient mechanism should be designed which will detect the attack before it gets terminated and limit down its effect. Sybil attack is the impersonation attack that forges identities of neighboring vehicles and through those identities; it injects false information in the network. This attack can be base for almost all other attacks and hence can even result in human life loss. Therefore, early detection of this attack will help in securing VANETS. In this report a mechanism is proposed that detects Sybil attack based on id and position of vehicles and also this detection mechanism is cost efficient as it does not require much extra hardware to be included for implementation. The detection rate offered by this mechanism is better than the existing mechanism. It detects Sybil attack at an early stage (online detection).

ACKNOWLEDGMENT

This report would not have been possible without the support of many people. Many thanks to my guide, **Mr. Ravinder Singh**, who guided me thoroughly, read my numerous revisions and helped in making some sense out of the confusion. Also thanks to the Lovely Professional University, Department of CSE for allowing me to pursue my dissertation in the topic of my choice.

And finally, thanks to my classmates, parents, and numerous friends who endured this long process with me, always offering support and love.

DECLARATION

I hereby declare that the dissertation II entitled **Sybil Attack Detection through Distance Calculation**, submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

The work was done under the guidance of Assistant Prof. Ravinder Singh, at Lovely Professional University, Phagwara.

Vaishali Aggarwal

Date: (Reg. No. 11301383)

CERTIFICATE

This is to certify that **Vaishali Aggarwal** has completed M.Tech dissertation II title under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation II is fit for the submission and partial fulfillment of the conditions for the award of M.Tech Computer Science & Engg.

Date: ……

Sign of Advisor
Name:
UID:

Table of Contents

List of Figures

Chapter 1

INTRODUCTION

1.1 VANETS

Many aspects of human life are revolutionized by rapid advancement of pervasive wireless communications and information technologies. Therefore, these technologies enable the development of wide range of applications and services that are of personal as well as public nature. A vehicular ad-hoc network (VANETs) is one such technology that provides vehicular communication. VANET is the first commercial implementation of MANETs (mobile ad-hoc networks). Great numbers of applications are supported by vanets that relate to vehicle traffic, vehicles, drivers, pedestrians and passengers, ranging from entertainment to traffic safety. It is a core constituent of next generation intelligent transportation systems (ITS) and consist of infrastructure acting as fixed nodes and radio-enabled vehicles acting as mobile nodes .In vanets, vehicles that are in range of 1000meters of range can communicate with other vehicles called as Inter Vehicular Communication(IVC) and with RSU's (Road side units) called as Vehicle-to-RSU communication(VRC). These vehicles can share traffic related messages, safety messages etc with each other. It basically considers vehicle safety, traffic management, driver assistance and infotainment. Figure1 shows a typical VANET structure. (Mahmoud Al-Qutayri, 2010)

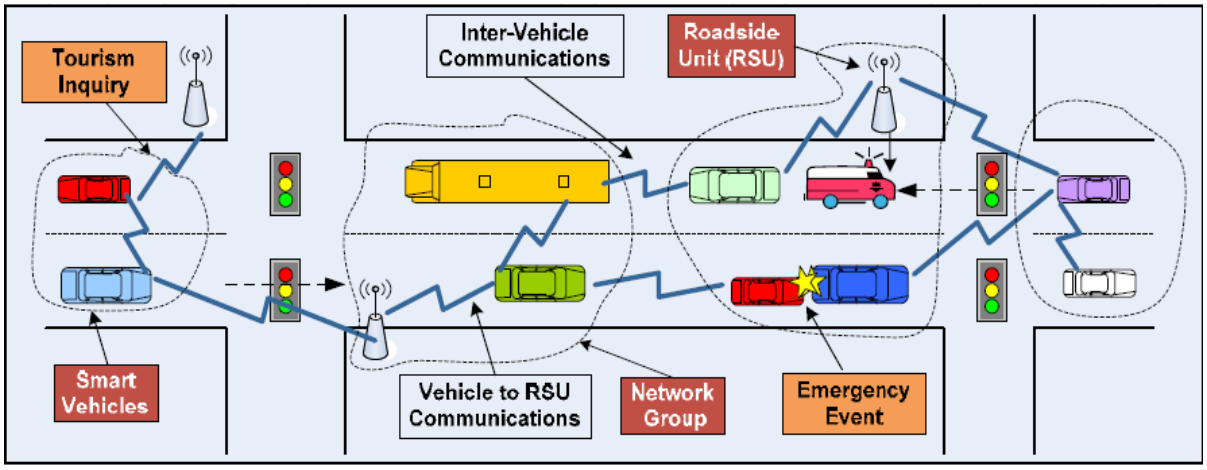


Figure 1: A typical VANET structure

Vehicles use DSRC (direct short range communication) to communicate with each other wirelessly. It can be both distributed as well as centralized network. With the VANET technology, now the vehicles are being called “Computer network on wheels”. Vehicles must have Event Data Recorder (EDR), GPS system, navigation system for storing information and getting location information about other vehicles. Rich resources and unlimited energy is available in VANETs. Continuous power is offered by engine of vehicle for GPS devices, communication or other devices. Inertial sensor or digital map can be installed in the vehicle and that can be used by the vehicle to obtain direction, velocity and location .Also vehicle can be made available with a high performance integrated chip to offer storage capability and strong computing power. (Jianqi Liu, 2015)

1.2 VANETS SECURITY

The VANET concept is still not deployed fully only because of security concerns. In VANET, vehicles make route selection decisions based on information received from other nodes. Being a wireless network, VANET is open to all security threats that are present in wireless systems. So a great care should be taken that the communication done is secure enough as it deals with human life. VANET if badly designed can open doors to various attackers. As all nodes are mobile, nodes stays in each other’s range for very small time, communications is done through wireless channel and data change is very frequent so any kind of malicious attacker should not be able to intervene in communication and disrupt the network and hence harm human life in any way. Vanets provides many safety and entertainment oriented applications such as traffic conditions update, accident reporting, internet access etc. It should be taken care of that any kind of emergency information concerning human lives should not be added or altered by attackers. Also privacy of drivers should we well protected. It is going to benefit people in many ways so its security should be the prime concern against the attacks. An attacker can attack the vehicular network for his personal benefits or with a view of bringing network down. There are various kinds of attacks possible as bogus information, routing, DOS, Sybil, timing, GPS spoofing, hidden vehicle attack. If any of these attack takes place than security of vanets is questioned because than attacker can inject any information, alter any information, track any other vehicle. In VANET, many voting based schemes are used for decision making. So, if attacker can easily

forge multiple identities then that decision can be easily changed and hence it will affect the normal behavior of VANET. Therefore, an efficient mechanism should be designed which will detect the attack before it gets terminated and limit down its effect. Sybil attack is the impersonation attack that forges identities of neighboring vehicles and through those identities; it injects false information in the network. This attack can be base for almost all other attacks and hence can even result in human life loss. Therefore, early detection of this attack will help in securing VANET. (Mahmoud Al-Qutayri, 2010)

1.3 TYPES OF ATTACKERS

There are different types of attackers present in the network that can be classified on the basis of behavior of attacks, scope and nature. Different types of attackers are-:

i. **Active Attacker:** This is the type of attacker that either doesn't forwards the received packets or forwards the packets after generating and adding wrong information in them.
ii. **Passive Attacker:** This type of attacker doesn't directly perform any activity in the network but just eavesdrop on the wireless channel to collect information about network that can be useful to other attackers.
iii. **Insider:** This type of attacker is a trustable/authenticated member of network and is having access to all public keys and also to other members of the group.
iv. **Outsider:** This type of attacker is not the part of network and is an intruder.
v. **Malicious Attacker:** This type of attacker doesn't seek any personal benefit from the attack. He just wants to disrupt VANET or harm other members of network.
vi. **Rational Attacker:** This type of attacker attacks for personal benefit and is predictable in terms of target and type of attack.
vii. **Local Attacker:** This type of attacker performs attack within in limited area.
viii. **Extended Attacker:** This type of attacker performs attack that is distributed across the network.

1.4 TYPES OF ATTACKS

Before designing a security mechanism for VANET, we must know about all possible attacks that can be performed by a malicious/rational, active/passive, insider/outsider attacker.

Below are the attacks possible in VANETs:

i. **Denial of service attack**: In this type of attack, attacker tries to bring down the network by jamming the signal or by flooding the network with spam messages.

ii. **Black Hole Attack** (Al-kahtani, 2012): In this the attacker vehicle, by showing low hop count and fresh route, tries to attract other vehicles so that they route packets through it. Once vehicles start routing packets through it, the attacker vehicle simply drops the packets.

iii. **Worm Hole Attack** (Al-kahtani, 2012): In this attack, there are two malicious vehicles and they both are at two ends of a network. Thus a tunnel is created between them to transmit data packets from one end to another end. Then these packets are sent (broadcasted) to the network. Once these malicious nodes take control of the small network connection they send false information to the network and afterwards delete these data packets.

iv. **Replay Attack**: It is also known as playback attack. In this attack the attacker vehicle overhears the communication of a two vehicles and captures some information in between. Then it resends (replays) the same information next time.

v. **Hidden Vehicle** (Maxim Raya, 2007): In this attack a vehicle that is in emergency situation and is broadcasting warnings for informing it to others, waits for a reply from neighbors and it gets to know that one of its neighbors(attacker vehicle) is in better condition to forward message, it stops broadcasting further messages. Now here attacker vehicle shows that it is in better condition and it will not forward any message to other vehicles.

vi. **GPS spoofing** (Al-kahtani, 2012): In this attack, attacker uses GPS satellite simulator to produce signals that are much stronger than the signals produced by actual satellite system. So through this attacker can change the GPS readings of the target vehicle and make them think that they are in different location.

vii. **Malware and Spam** (Al-kahtani, 2012): Attacker performs this attack on On-board-Units (OBU) and Road side units (RSU). They perform these attacks by inserting spam or viruses when OBU's and RSU's perform software updates.

viii. **Bogus information** (Al-kahtani, 2012): In this type of attack, attacker transmits the wrong information in the network for his own benefit as road clearance etc.

ix. **Timing Attack** (Al-kahtani, 2012): In this type of attack, timeslots are added into the original emergency message, by the malicious vehicle. Thus messages are not transmitted at the right time to the neighbors which is otherwise very important in VANETs.

x. **Sybil Attack**: In this attack, the malicious vehicle either creates fake identities or spoofs the identities of neighboring vehicles and uses those identities to send messages to a target node and take benefit out of it.

1.5 SYBIL ATTACK

Sybil attack is an impersonation attack in which a malicious vehicle/Sybil attacker generates fake identities or steals the identities of honest vehicles (which are then called Sybil nodes) during vehicular communication. In this attacker forges the identity of the honest vehicles and communicates with target vehicle with those identities, where target vehicle thinks that it is receiving messages from different honest vehicles where as in actual it is one single vehicle who is having multiple identities is communicating with target vehicle. An honest vehicle can have only one unique identity in a network. An illusion is created by the Sybil attacker and through that illusion of multiple identities it injects false information into the network in order to disrupt the network. This attack can also help attacker to launch almost all other attacks, as for example, when there are more than one Sybil attacker and all after forging multiple identities sends messages at a same time can bottleneck the network and hence can bring network down. Thus, resulting in a DOS attack. (Parastoo Kafil, 2012)

Following is the categorization of Sybil attack:

i. Attack done through identity stealing: In this the malicious node steals the identities of honest nodes (Sybil nodes) and shows that identities to be original identities (means shows that those are honest nodes).

ii. Attack done through generating fake identities: In this malicious vehicle generates fabricated identities that belong to real network but that identities don't exist at all. It generates these identities through network identity generating algorithms. (Parastoo Kafil, 2012)

A real time example of a Sybil attack can be as: when a vehicle wants to clear its way out of traffic it can use Sybil attack to do this as it will spoof identities of neighboring vehicles and

then send a message of route change to all honest nodes through these fake identities. Now honest nodes will think that same message is coming from multiple nodes so it is legal message and hence it will change its route. This way malicious vehicle will clear out its way in traffic area. Below is the diagram representing Sybil attack in VANETs.

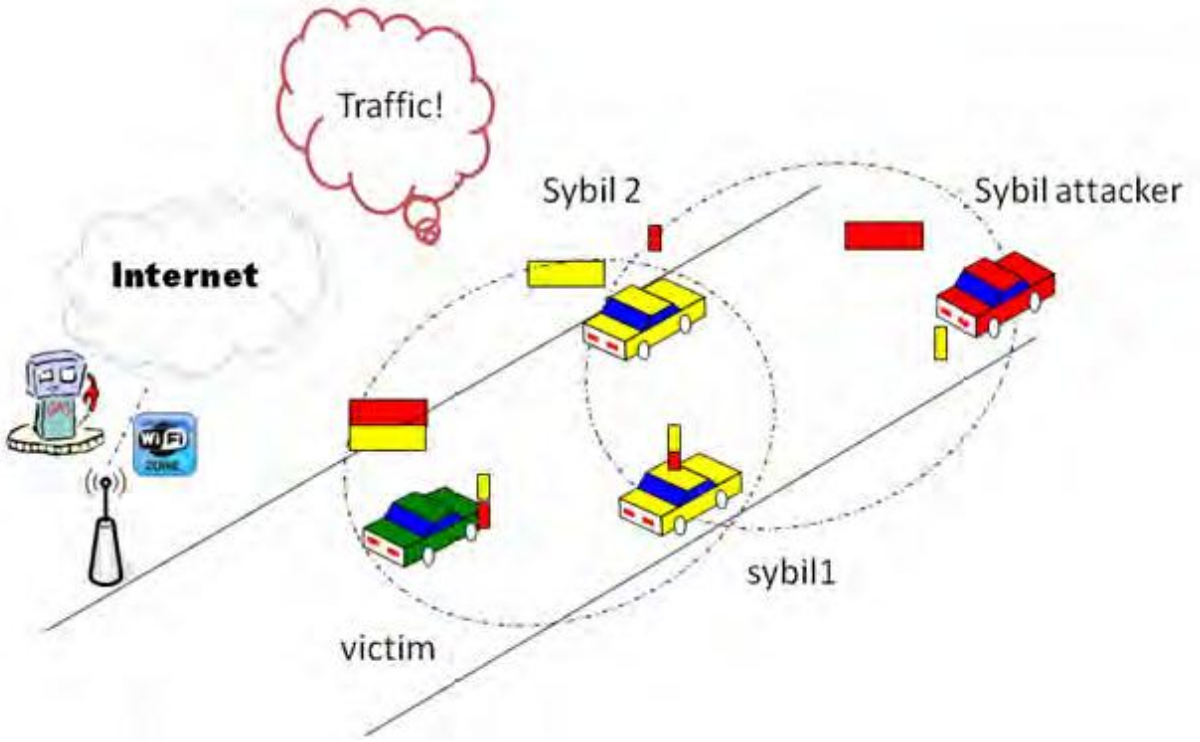


Figure2: A picture of Sybil Attack

In Figure2 Sybil attacker (red vehicle) clear outs its way by forging the identities of two Sybil nodes (yellow vehicles) and misguides the victim node (green vehicle) by sending the false message (to change the route due to traffic) from the forged identities. And victim node thinks that multiple vehicles are sending same message so it changes it routes. (Parastoo Kafil, 2012)

Also attacker can plan such events through this attack that can cause human life loss. This attack makes vehicular network insecure.

1.6 EVOLUTION OF SYBIL ATTACK

Sybil attack is an impersonation attack which was first discovered by John R.Douceur in peer-to-peer systems. This attack was named after a book named “SYBIL”. This book

contained the case study of a woman who was diagnosed with “dissociative identity disorder” also known as multiple personality disorder. This disorder means that one person shows different personalities/identities due to memory damage. Same is the action performed by a Sybil attacker during attack. He forges the identities of other neighboring vehicles and then uses those identities to make the target vehicle believe that message is coming from different vehicles and hence target vehicle makes his routing decisions based on those messages. Whereas those message were sent by a single vehicle that is Sybil attacker only. And hence Sybil attacker gains the maximum benefit in the network. In vanets attacker misused the fact that identities of vehicles are open and through these identities he can easily track locations of vehicles and hence use it to misguide anyone in the network.

Chapter 2

REVIEW OF LITERATURE

Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, Stephan Olariu, (2007), proposed the approach that considered position security of vehicles. The approach used the on board radar in the vehicles in order to detect the position of the neighboring vehicles. This way it achieves the position security locally and globally. Vehicles are assumed to have GPS maps and GPS receivers, a rear and front radar. A position attack takes place when attacker vehicle's GPS position is changed. Sybil attack takes place when a vehicle spoofs other vehicle's ID. These two attacks can happen combined also. Radar is used to get the position, angle and velocity of the vehicle. In this approach, when verifying vehicle did not receive any message from the verified vehicle for a long time then it increases the time out counter by one. GPS position values and radar values are extended little and the position is located that lies near to both values. If that position is found than GPS position is correct otherwise vehicle is a suspected vehicle. Now vehicles lying at nearby GPS positions are grouped together. Now as these vehicles will face same traffic conditions, so if there is any malicious vehicle present that is changing message, it can be detected by honest nodes. Every vehicle knows the position of its neighboring vehicle from the messages it exchanges. Now after analyzing position data, a map history is created from it and stored in vehicles. A vehicle is trustable only if it has map history stored in it. Map history tells about the movement criteria of the vehicle, so whenever any position message is heard from any vehicle, verifier vehicle first checks its position from map history. (Gongjun Yan, 2007)

Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, Bertrand Ducourthial, (2008), proposed a mechanism that uses the node's localization to verify the authenticity of communicating nodes.Also for determining Sybil ad malicious nodes , an estimated metric of the degree of distinguishability between two nodes is defined. This scheme detects sybil node based on the signal strength received from forwarding node and the GPS position that it adds in message. Node matches both and mismatch occurs then it means that forwarding node is a Sybil node. Here assumption is made that all messages are having same signal power. All process takes place in two steps. First is comparing future geographical localizations with

evaluated localizations and once node is suspected then second step is followed to confirm the suspected node. In second step in order to detect sybil and malicious node, sybil detection mechanism is launched by every vehicle in network. (Mohamed Salah Bouassida, 2008)

Kevin C. Lee, Uichin Lee, Mario Gerla, (2009), presented the difference between different VANET protocols. This paper shows how GPSR(Greedy Parameter Stateless Routing) protocol is better than AODV(Ad Hoc On Demand Distance Vector) protocol for VANET. The packet delivery ration of GPSR protocol is much better than AODV in the case when density of vehicles increses in both highway and city scenario. Hence increasing the overhead in AODV protocol and becoming much more higher than GPRS. As local maximum rarely happens on highway therefore, GPRS is favoured for highway scenario.Even with the increase in communication distance, the packet delivery ratio remains close to 100%. In greedy mode in GPSR, the immediate neighbor which is also geographically closer is being forwarded the packet by the preceding node. There is also a perimetr mode in GPRS in which it recovers from local maximum based on right hand rule. (Kevin C. Lee, Oct 2009)

Tong Zhou, Romit Roy Choudhury, Peng Ning, Krishnendu Chakrabarty, (March 2011) presented a scheme in which large number of pseudonyms are assigned to vehicles. Two hash functions i.e. Coarse grained (Hc) and Fine grained (Hf) are used to group pseudonyms. A unique fine grained Hf (pi/kf)and coarse grained Hc (pi/kc)hash values are assinged to each pseudonym where kf , kc are freshness keys and pi is the ith pseudonym. Pseudonyms belonging to different nodes must be having different fine grained hash values. A check is performed by RSU to know that if two pseudonyms hash to same value of coarse grained. If yes then it means that these values are from same vehicle or two different vehicles are having same coarse grained value. Then RSU informs about this to CA and then CA checks for the Sybil attack. (Tong Zhou, March 2011)

Mina Rahbari, Mohammad Ali Jabreil Jamali, (Nov 2011), presented a method for detecting Sybil attack which is based on fixed key infrastructure. He has used an encryption technique that gives four security aspects and also detects attack. Authentication: In order to

authenticate the vehicle, author has used two types of certificates, valid and adversary certificate. Valid certificate is given to the valid vehicle and adversary certificate to the malicious vehicle. Whenever a vehicle asks for a key or sends a message, it will be provided the needed data only if it has valid certificate. Non-repudiation: So author has given a concept of Centralized authority(CA) that will provide the vehicle its public key and whenever vehicles sends any message it encrypts the message with CA's public key and now only CA will be able to find out identity of vehicles with its private key in emergency situations and no one else in the network. Privacy: Author has used private key concept to keep this info secure. Data Integrity: Author has used a technique to make sure that received data has not changed or modified in between. That technique is HMAC (hash message authentication codes). HMAC is used to sign the sent packet to make sure that information is not changed. Two centralized authorities (CA's) are used. One CA keeps the local key and other CA holds the initial certificates and the vehicles information. As paper has used certification mechanism so detection delay is low.

The drawback of this scheme is that it finds only Sybil community but not malicious node. Also it has another problem that if nodes move to other region that it this mechanism will not be able to detect Sybil attack. (Mina Rahbari, 2011)

Soyoung Park, Baber Aslam, Damla Turgut, Cliff C. Zou, 2011, proposed a method based on timestamp series approach against Sybil attack. In this approach RSU is itself assigning certificates. It targets the initial deployment stage of VANET when less number of vehicles are prsent and a basic RSU support is available. Two can't pass through same RSU at same time. With this assumption, if two vehicles are sending messages with same timestamp then it is considered to be attacker vehicles. This approach neither require internet based RSU's and not public key infrastructure based vehicles. But the problem with this approach is that if RSU is compromised then it will not work. (Soyoung Park, 2011)

Yong Hao, Jin Tang, Yu Cheng, (2011), proposed a security protocol that will used to detect attacks in position based applications. This technique uses the GPS positions of vehicles that are given in the communications messages, to detect the attack. Two system models i.e. network model and security model are used. In network model, It is assumed that

each vehicle is equipped with DGPS technology and an on board unit (OBU). Then it checks the validity of vehicles position with respect to its neighbor's position. In security model, security is provided against active, inside and rational attackers. For providing privacy to vehicles, short group signature technique is used. It works in three phases as: probing, confirmation and quarantine. In Probing phase, the vehicle will transmit safety message with its geographical location and also with indexes of nearest M vehicles. Nearest M means, M number of vehicles in front and M number of vehicles at back. Index value can be any value that will uniquely identify a vehicle. In confirmation phase, many vehicles are sent to the both sides of suspect vehicle named as S and O. Whenever any action is suspected than S nodes will generate a warning message with the suspected vehicle's index value and encrypt that message with its partial private key. When threshold value of S vehicles confirms attack that it is declared that suspected vehicle is attacker otherwise the O nodes on other side will check the same by comparing the distance between the suspected node and S nodes with suspected node with O nodes. If distance is more than O nodes confirms the attack. Then signatures are generated by verifying vehicles which is complete will confirm attacker otherwise it is considered that it is not an attacker. Drawback of this protocol is that it will not be able to detect multi-Sybil scenario. (Yong Hao, 2011)

Nicole El Zoghby, Veronique Cherfaoui, Bertrand Ducourthial, Thierry Denœux, (2012), proposed a method known as distributed data fusion for detecting Sybil attack. In the belief function framework the distributed confidence over the network is being built by this algorithm. The exchanged message contains the sender's confidence on the network nodes. Each node can assign confidence to every other node of network. If confidence is 0 then it means that it is fake node and if it is 1 then it means that it is real node. Nodes save two kinds of information i.e. local knowledge and public knowledge. Nodes combine local and public knowledge and then broadcast the final results to network to tell them exact confidence on all nodes. The problem with this approach is that it doesn't consider the contents of message.(Nicole El Zoghby, 2012)

Parastoo Kafil, Mahmoud Fathy, Mina Zolfy Lighvan, (2012), this paper describes that what all models can be used by an individual Sybil attacker. There can be basically three categories in which Sybil attacks can be arranged:

i. Communication: There can be direct communication between Sybil attacker and legal node or there can be indirect communication. In direct communication, legitimate node directly talks to Sybil nodes whose identities are stolen by malicious node. And in indirect communication, legal node is able to communicate with Sybil node through Sybil attacker.

ii. Identity: There are two ways in which malicious node can generate its identity. Firstly it can generate fake identities that do not exist at all in the network through identity generating algorithm. Secondly by stealing the identities of nodes in its vicinity.

iii. Participation: An attacker can use all of his identities at once means same time or he can use only one identity at once. It is his wish.

There are various traffic models available for knowing Sybil attack as: Highway Model, Uniform Model and Urban Model

The format of a packet send by Sybil Attacker (SA) is as: (Parastoo Kafil M. F., 2012)

Sybil ID is the source ID	Sybil position is the source position	Hop count	Destination ID	Sybil Seq#

Figure3: Format of packet sent by SA

Rasheed Hussain, Sangjin Kim, Heekuck Oh, (2012), Presented privacy preserving warning and beaconing mechanism. Hybrid mechanism is proposed that will handle Sybil attack as well as misbehavior in VANET. Here author has considered an attacker to be an insider with more capabilities and resources than an honest node. Traffic density is calculated based on scheduled beacons and virtual ears (beacons) and virtual eyes (radar) are used to verify location information. Beacons that will not reveal identity are used for signature based scheme and privacy of warning messages. Post warning measurements are checked for immediate source of warning message. The normal expected behavior is matched against recorded measurements and action that is expected after warning is stored in on board units of vehicles. To check the correctness of information opposite traffic is used. Author has covered two cases that includes dense traffic situations and sparse traffic situations and thereby uses Sybil attack detection scheme and Location based misbehavior detection

scheme. (Rasheed Hussain, 2012)

Mohammed Saeed Al-kahtani, (2012), this paper describes various security attacks possible in VANETS and their detection mechanism. There are several security requirements as-: authentication, data verification, availability, Non-repudiation and privacy. There are various kinds of attackers available in network as rational and malicious attackers, outsider and insiders, passive and active attackers. A rational attacker looks for his personal benefit from the attack whereas malicious attacker doesn't want any kind of benefit for himself. Outsider is the attacker lying out of range of vehicles and insider lies in the network range. Passive attacker cannot modify any information but can only read information where as active attackers can completely change information. Various types of attacks possible in VANETS are-: Denial of service attack, Black Hole Attack, Worm Hole Attack, Bogus information, GPS spoofing, Malware and Spam, Timing Attack, Sybil Attack. These are various attacks that can hamper the security of vanets. So, right defense mechanism should be used to overcome this. (Al-kahtani, 2012)

Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, Xuemin (Sherman) Shen, (June2012), proposed a Sybil detection mechanism that considers the location privacy and it provides it by use of trajectories of vehicles. There are three actors (TA, RSU, Vehicles) to be considered. (TA)Trust authority will take care of all RSU's. It generates a public private pair of keys and shares its public key with all RSU's. TA's public key is used by RSU's to verify that a message is authorized by TA. RSU signatures consist of three parts. POK (proof of knowledge), Event id and link tag. When an event expires, all RSUs in the system simultaneously compute a new event id and link tag for the next event (next period of time). When RSU sends an authorized message to a vehicle, at the same time it sends the same link tag to its neighboring RSU's also. It helps neighbor RSU to verify vehicle's identity. Whenever any vehicle v1 comes in network of RSU1, RSU1 generates an authorized message for v1 and sends it to v1 with its signature on it. At the same time it sends the link tag of that message to neighbor RSU's also. Now when vehicle goes into RSU2 range, it first sends its authorized message received from RSU1 to RSU2. RSU2 verifies the link label of RSU1 by comparing it with the link label send by RSU1 to RSU2. If link label don't match

then that means vehicle is malicious. Now when v1 passes any message to v2, it passes the trajectories (which is the sequential authorized messages i.e. M1, M2, M3, M4, M5). Now v2 will check for the sequence of messages in each trajectory. A malicious vehicle will form multiple subsets of this trajectory and hence use it to show its multiple identities. (Shan Chang, 2012)

Mukul Saini, Kaushal Kumar, Kumar Vaibhav Bhatnagar, (2013), presented different methods possible to detect Sybil attack. It defines the architecture of VANETs which includes department of motor vehicles, road side units and nodes/vehicles. Then is discusses different possible threats to VANETs that includes eavesdrop on wireless messages, re-broadcast and modifying messages, Replaying messages at different location and time, impersonating other vehicles, compromise RSBs, Sybil attack and message suppression. Various detection techniques available are-: Resources testing, use of public key cryptography, assumption of propagation model, secure positioning, distinguish ability, signal strength based position verification, claimer and witness (Mukul Saini, Nov 2013).

Kenza Mekliche, Dr. Samira Moussaoui, (2013), proposed an approach to detect Sybil attack by using infrastructure and localization of nodes. This is a privacy preserving approach which uses neighbor RSU's for knowing the location of the suspicious node and calculating the difference in the positions of these malicious nodes. In this approach DMV (Department of Motor Vehicle) is the centralized authority that manages all RSU's. Pseudonyms are assigned to each vehicle by DMV. These pseudonyms are the secret identity of the vehicle which identities a vehicle uniquely in the network. These identities are provided after hashing the original ID with one way hash function. Two keys are used to hash this value i.e. coarse grains and fine grains.

This approach works in three steps:

Initialization step: In this step pseudonyms are assigned to vehicles by DMV. Firstly pseudonyms are hashed with one way hash function and then result is sent through filter that creates hash collision and coarse grained pseudonyms by using key Kc. Now again this is sent to another filter which creates fine grained pseudonyms by using Kf key.

Sybil Attack Detection step: RSU will maintain a list of pseudonyms with the position of

each vehicle after overhearing the vehicles communication. Now RSU will first match the pseudonyms to see that which pseudonyms lie in coarse grained group. Now it confirms the position of each suspicious node by calculating RSS and angle of arrival. After calculating their positions RSU calculates the probability of nodes being malicious and reports it to DMV.

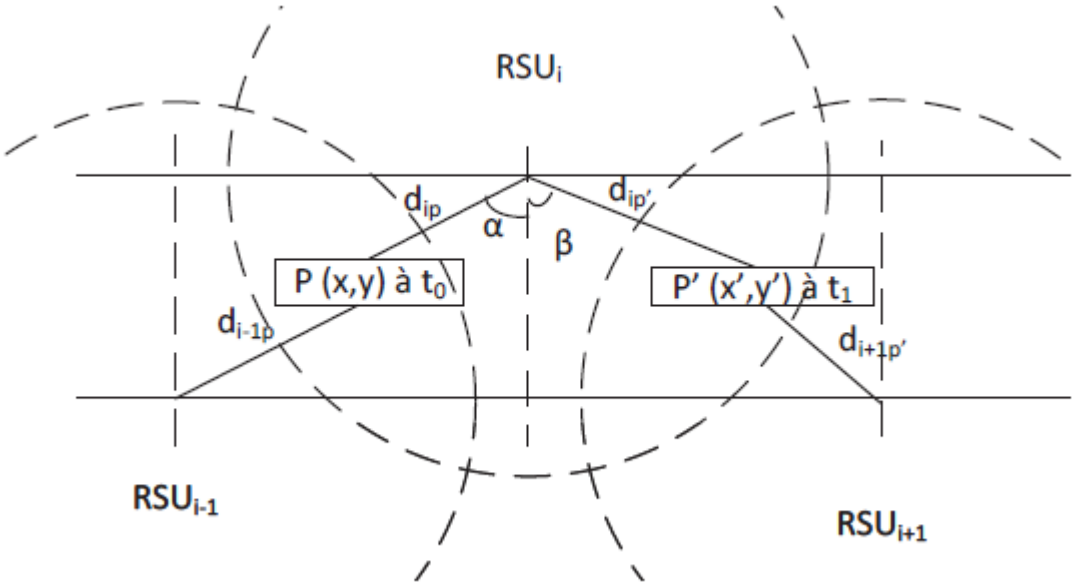


Figure4: Node Localization

Verification Step: Now DMV uses Kf to know that if the suspected nodes (as informed by RSU) belongs to fine grained group. This approach is though reducing workload of DMV but it uses large number of RSU's. (Kenza Mekliche, 2013).

Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali, (2013), this paper describes various challenges in the security that are being faced by VANETS. The major security challenges in VANETS are privacy. Privacy preservance of both driver and vehicle is required. With the personal privacy, the location privacy is also very important in VANETS as the attackers mainly target the position and identities of vehicle for injecting wrong information in the network.

Second security issue is the scalability problem. The network of VANETS is dynamic in nature. It continuously keeps on changing due to node mobility. So scalability problems should be solved in such a way that honest nodes are not intimated about it.

Third is the trust which is most important challenge as VANETs is all about routing information received from other members. So it is all about how much a vehicle can be trusted in a network to accept it information.

Forth one is the consumers. With the increasing security mechanisms, the cost of hardware is also increasing. Cost here includes cost of road side infrastructure, cost of technical support etc.

So while designing any security mechanism all these challenges must be kept in mind for a successful mechanism design. (Mostofa Kamal Nasir, 2013)

Bayrem Triki, Slim Rekhis, Mhamed Chammen, Noureddine Boudriga, (2013), proposed a Sybil attack prevention and detection mechanism in which two techniques for authenticating the identities of vehicles is used. One is RFID tags and other is certificates. RFID tags are present inside the vehicles and they are used to authenticate vehicles to RSU and thus get certificates that have short lifetime. Certification authority is used to assign certificates to RSU and vehicles. Certificates are used by vehicles to authenticate their identities to the neighbors. This approach considers that there are various certification authorities that are assigned to different regions. Here network is divided into various zones. And each zone has RSU and RSC (road side controller). Whenever a vehicle enters a new zone then it has to get a new certificate as per new region's certification authority. With the vehicles even the RSU's are also authenticated by CA. Through this approach attackers will not be able to track the position of vehicles. Now it is possible that a vehicle gets a certificate from one zone and then it enters another zone and gets another certificate. But immediately it returns back to old zone. So in that case it has two certificates with it now and both are valid. Now this vehicle will be able to perform Sybil attack as it is having two valid certificates with distinct ID's. So it important that whenever vehicle enters new zone, its old zone certificate should be made invalid. This is done by RSU. RSU generates a certificate revocation request to RSC and thus forwards the list containing the list of certificates revocated to all vehicles. Now neighbor vehicles can easily know that attack is happening

and thus inform RSU. The certificate will be having the identity of a vehicle in a secret form so that it can't be forged by another vehicle.

Also Sybil attack can happen as certificates from two different zones can be used or new certificate is not provided to vehicle yet because of non-range area or there is problem in reading vehicle's tag due to communication issues. So to confirm it, an alert message is sent by RSU to RSC. It asks from RSC that if vehicle has got certificate from the zone it is lying now. And then it checks from neighbor RSU that if vehicle has got new certificate. If all these conditions are true then RSU confirms Sybil attack and generates a report and sends to RSC and all other RSU's. This approach provides privacy protection and is very efficient in detecting Sybil attack.

The drawback of this approach is that it is considering many centralized authorities which will add up for delay in detection process. (Bayrem Triki, 2013)

J.Grover, V.Laxmi, M.S. Gaur, (2014), proposed a technique that is based on the fact that Sybil nodes (fake nodes) and malicious node shares the same neighbors nodes. Thus without using secret information exchange and special hardware Sybil attack can be detected easily and quickly. Here assumption is made that RSU's can't be compromised due to its isolated location and tamper proof capabilities. Two types of neighbors are considered. One is physical and other is communication. This is basically done to detect any change in transmission power by any vehicle. RSU doesn't come in picture in this methodology and all detection is done by vehicles itself by creating group of neighbors after regular time intervals. But it doesn't detect Sybil nodes when they can use variable transmission range. (J.Grover, 2014)

Ali Akbar Pouyan, Mahdiyeh Alimohammadi, (2014), surveyed on three methods for detecting Sybil attack and compares them. There are three methods of detecting Sybil attack:

i. Resource testing: In this method, the vehicle is tested for resources like memory and computational, radio and identification resources. When a vehicle wants to test radio resources of a target vehicle, it sends a message to all vehicles and selects a particular channel for receiving a reply. Now if attack is taking place then attacker would not be able to send reply at different channels at same time but if node is legal one then it

will reply on same channel at same time. But this method is not so useful as an attacker can have now multiple channels to reply from.

ii. Position verification: This mechanism uses the fact that a vehicle's present location can only be a unique position. A vehicle cannot be present at more than one location at a particular time. There are various methods to verify position which includes range free and range based methods. Range based methods include RSSI (Received Signal Strength Indicator). From the two, range based method are much more useful. Benefit of this method is that there is no need to employ extra equipment. It should be taken care of that vehicle position should be confirmed from two ways in order to get correct information.

iii. Encryption and authentication: These methods use symmetric and asymmetric cryptography techniques to detect Sybil attack. But these techniques are much more time consuming and they have more overhead of generating, sharing and maintain keys. Symmetric technique is much better than asymmetric in terms of resource usage. (Ali Akbar Pouyan, 2014)

Thiago M. de Sales, Hyggo O. Almeida, Marcello de Sales, (2014), proposed a Sybil attack detection and privacy preserving authentication protocol which is called m-k-anonimity. This proposal works in three phases namely-:registeration phase, temporary identity assignment phase and Sybil detction phase. In registeration phase, CA assigns group sign key, group public key, digital certificate of RSU and CA to vehicles. Cryptographic asymmetric keys and their certificates are used as vehicles identities. RSU checks for the vehcile's authenicity after vehciles negotiates temporary keys with RSU. Sybil attack is detected as if the neighboring vehicles belong to same set of anonymity then they will attach and send in the beacon the next digital certificate belonging to deeper anonymity set. The problem here comes with managing certificates. (Thiago M. de SALES, 2014)

P.Vinoth Kumar, M.Maheshwari, (2014), proposed a Priority Batch Verification algorithm which provides emergency vehicles with immediate response with less time delay. It classifies the requests obtained from multiple vehicles in order to provide immediate response.Timestamps that are provided by RSU are restricted at early stage in order to

prevent Sybil attack. In order to prevent attack, RSU uses the timer while assigning timestamp to particular vehicle. So now if vehcile demands for another timestamp before expiry of RSU's timer than RSU denies it with th possibility of that vehicle being the attacker vehicle. For serving emergency vehicles, the proposal is to check for identities. The vehicle's unique identifier is checked for

knowing that it is emergency vehicle or not. If its emergency vehicle than it is being serviced without delay. The problem with this solution is that this algorithm takes more computational time. (P.Vinoth Kumar, 2014)

Chapter 3

PRESENT WORK

Studied the research papers which are mentioned in the references and the problem is defined and then factors are selected on the basis of which attack detection is to be improved.

3.1 PROBLEM FORMULATION

Sybil attack is performed by attacker by showing multiple identities to a target vehicle. Now these multiple identities can be generated in two ways-:

1. Sybil attacker steal identities of neighboring vehicles: In this, attacker monitors its neighbor vehicles and spoofs its identities and then sends messages to target vehicle through these identities. In Figure 4: Sybil attacker spoofs ID's of vehicles s1, s2, s3 and uses these identities to send false messages (traffic ahead so change your route) to victim node. Victim node thinks that messages are coming from s1, s2, s3. But ideally messages are sent by Sybil attacker through ID's of Sybil nodes.

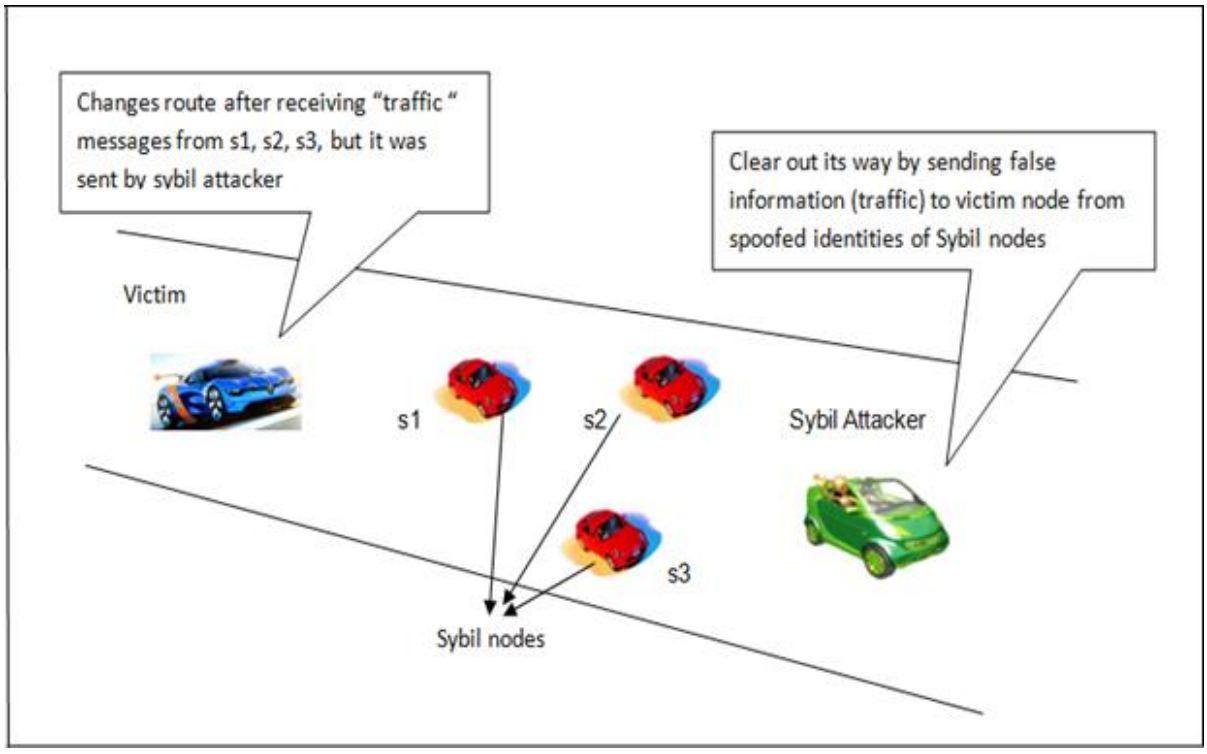


Figure5: Sybil Attack with spoofed ID's

2. Sybil attacker generates Fake identities: In this, attacker generates fabricated identities that don't exist at all in the network. It generates these identities through network identity generating algorithm. In Figure 5: Sybil attacker creates fake ID's s1, s2, s3 and uses these identities to send false messages (traffic ahead so change your route) to victim node. Victim node thinks that messages are coming from s1, s2, s3. But ideally messages are sent by Sybil attacker through ID's that don't exist at all.

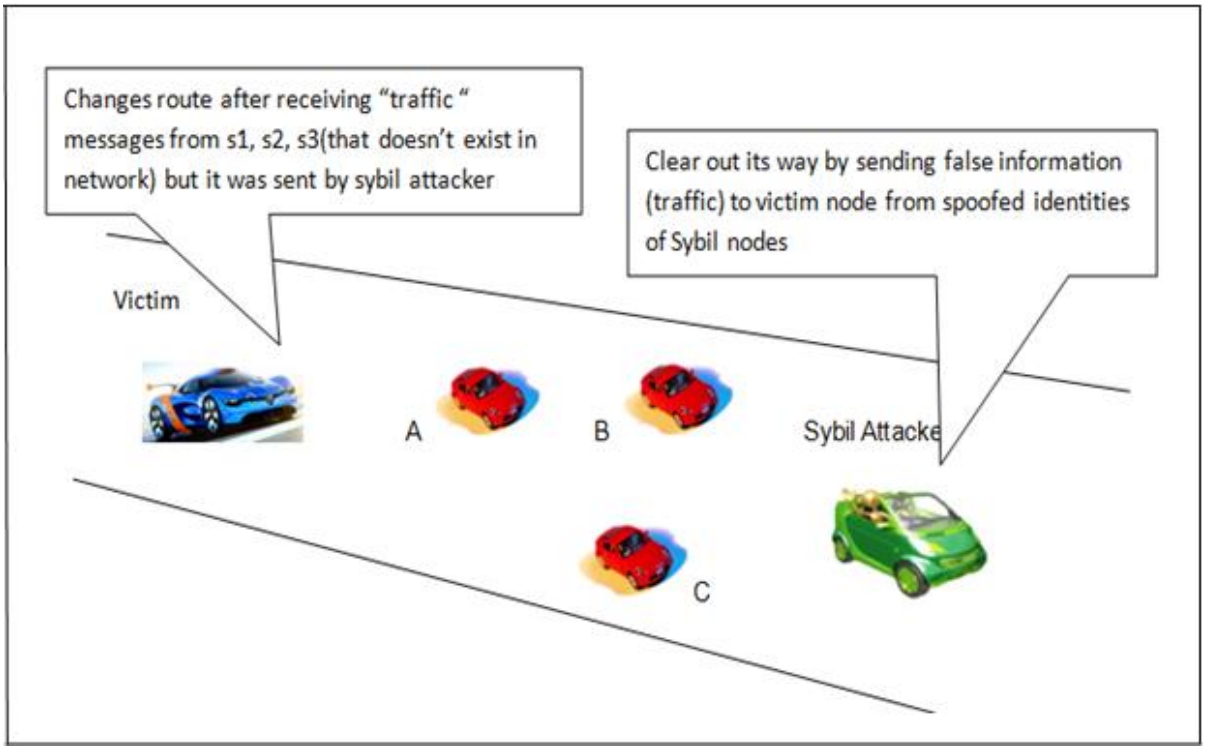


Figure6: Sybil Attack with Fake ID's

Now as the attack is defined with two possibilities, the main factors to be improved with this methodology are-:

- Detection Rate
- False positive Rate
- Cost Efficient Scheme
- Detection Time

3.2 OBJECTIVES

1. To detect Sybil attack before its termination which is also called online detection. Detection mechanism should detect attack before attacker can achieve its purpose.
2. To detect the Sybil attack by using as minimum resources as possible.
3. To detect the attack with the low delay possible.
4. To achieve better detection rate.
5. Reduce the false positive rate.
6. Attack is detected independently means no groups are to be formed in order to detect attack. This will avoid possibility of that attacker is attacking against the detection itself.

The main focus of the methodology given is to reduce the false positive rate, to improve detection rate, to reduce the detection time and to design the cost efficient mechanism. The cost is reduced as there are only two actors involved here namely-:

- Road Side Units (RSU's)
- Vehicles

As mentioned in literature survey, existing methodologies used Department of Motor Vehicle (DMV)/Certification Authority (CA), cryptography concepts. Inclusion of DMV and CA added extra cost to infrastructure and usage of cryptography concepts involved delay in detecting attack. The given methodology will eliminate all these problems.

3.3 METHODOLOGY

The detailed mechanism considers highway scenario. There are some assumptions are made while designing the below given system model.

3.3.1 SYSTEM MODEL AND ASSUMPTIONS

In VANET, vehicle can communicate with other neighboring vehicles through inter vehicle communication and with RSU's through roadside to vehicle communication. This mechanism considers highway scenario and requires each vehicle to be equipped with

necessary hardware i.e. On Board Unit (OBU). The components of system model as shown in Figure 7 (Shan Chang, 2012) are-:

- **Road Side Units (RSUs)**: Also known as wireless access points which provides user with wireless access within its coverage. Different RSUs are connected through internet or by a dedicated network thus resulting into RSU backbone network. Intersections are the points where these can be deployed. Bus stations and parking lot entrances are the other areas of interest where these can be deployed. Number of RSUs deployed is considered crucial in order to reduce cost. Therefore intersections are considered. RSU is placed on an intersection that is at acceptable distance from other intersections having RSUs and it is having maximum volume of traffic then other intersections without RSUs.

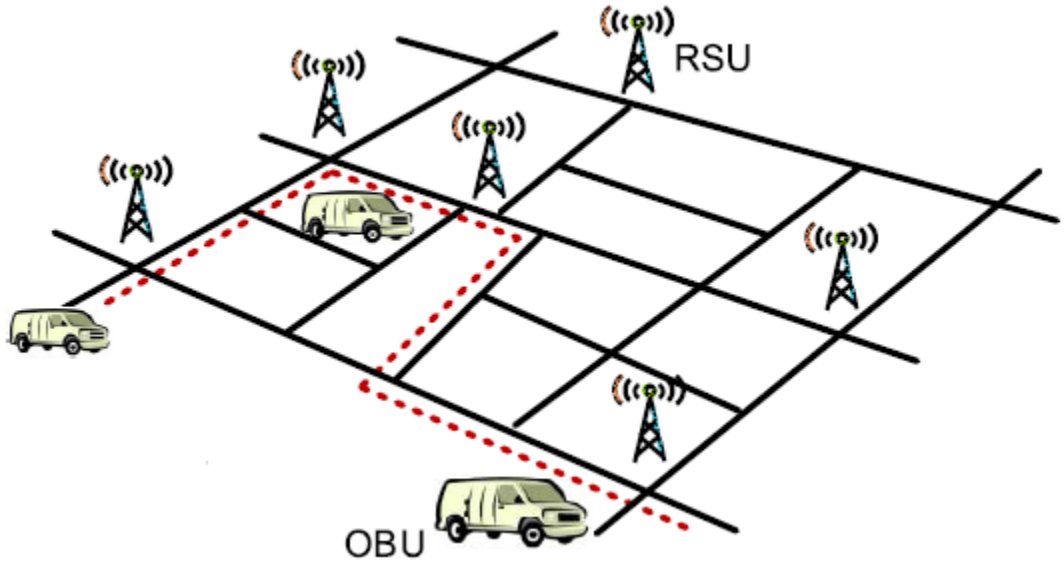


Figure7: An illustration of travel route of vehicle (dashed line) and different RSUs encountered by vehicle during its journey.

- **On-Board Units (OBU)**: It is the hardware that is installed within the vehicle. It generally have DSRC IEEE 802.11p module which is short-range wireless communication module and a GPS receiver. It is this hardware unit that enables roadside and inter-vehicular communication via wireless connections.

The below assumptions are made while designing the system-:

ASSUMPTION 1: All RSUs are fully trustworthy.

ASSUMPTION 2: Movement of vehicles is independent.

3.3.2 SYSTEM DESIGN

The presented design works in two phases namely: Initialization Phase and detection Phase. In initialization phase every vehicle registers itself to RSU and RSU saves its current location to its database. In detection phase RSU detects the attack at the time when vehicle confirms ID if neighboring sender from RSU.

(INITIALIZATION PHASE)

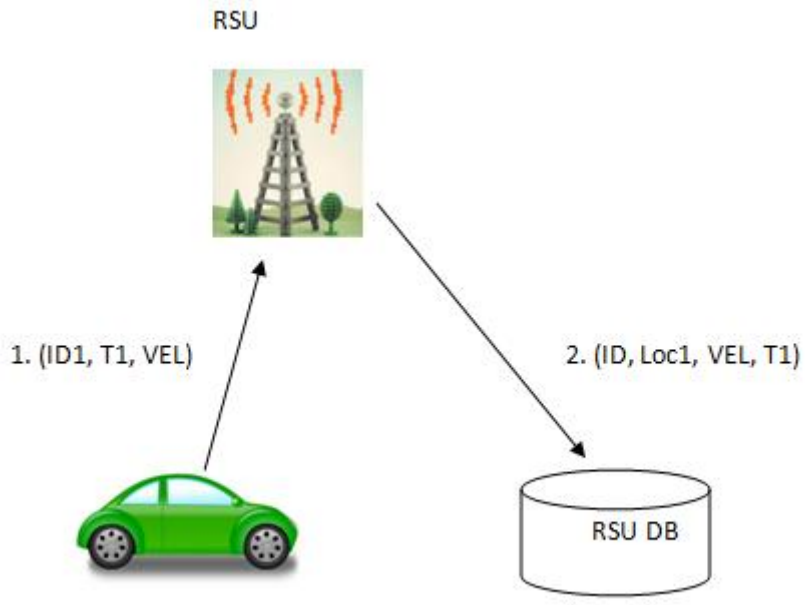


Figure 8: Initialization phase

i. As already mentioned, RSU's (Road side units) will be placed at intersections. Intersections are the points that are chosen based on distance from other intersection point and at the point with highest traffic.

ii. Vehicles are moving independently on highway. Whenever any vehicle enters in range of any RSU, it registers itself to RSU by sending below information to particular RSU: (ID, TIMESTAMP (T1), VELOCITY (VEL)

iii. RSU calculates approximate position (Loc1) of that vehicle using RSSI and saves this information in its database. If the ID already exists then it updates its database with current information.

(DETECTION PHASE)

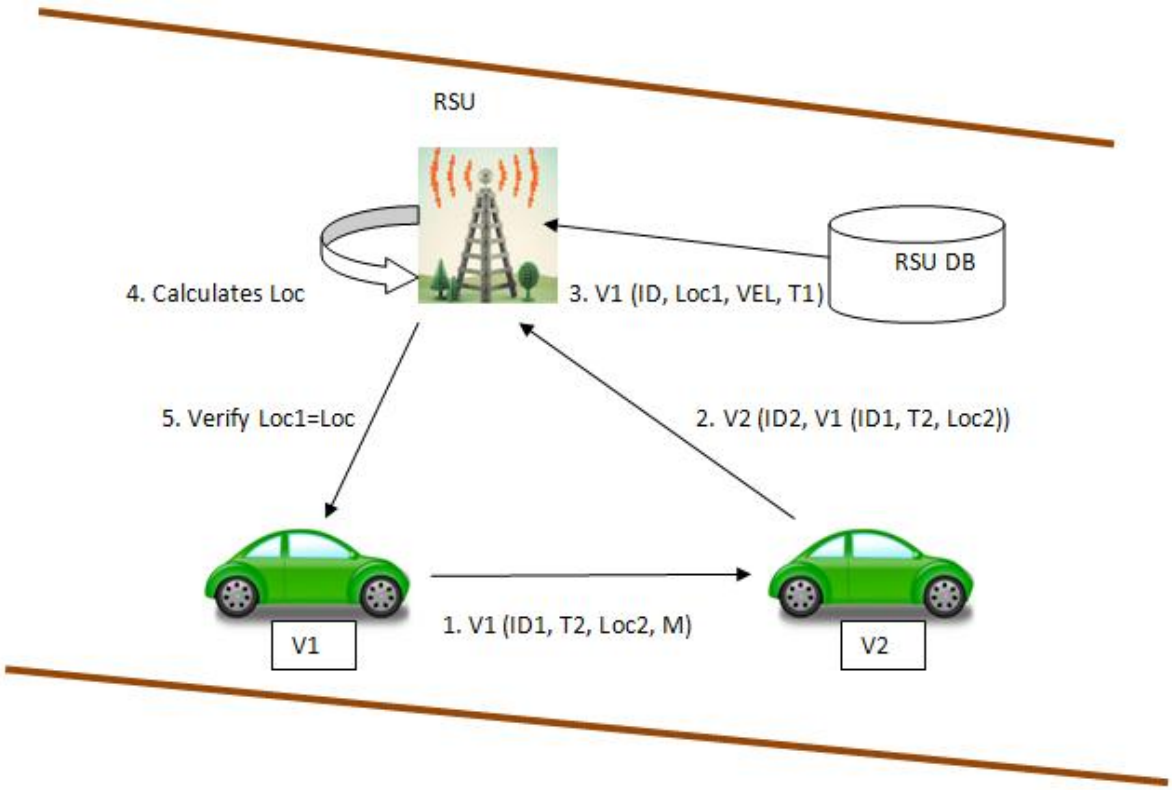


Figure 9: Detection phase

i. A vehicle communicating with other vehicles will communicate by sending its below details: (ID, TIMESTAMP (T2), MESSAGE (M), LOCATION (Loc2))

ii. Another vehicle (V2) before accepting this message gets the ID of sender verified from RSU. It sends V1 (ID, T2, Loc2) to RSU.

iii. RSU after receiving this information checks its DB for V1's ID and then calculates the approximate current location of the sender. Calculation of location is done based

on timestamp when vehicle registered to that particular RSU, its speed and timestamp of message send by sender to target vehicle. It is calculated as-:

- At Time T1 vehicle V1 location is Loc1 as calculated by RSU
- At Time T2 LOCATION of vehicle V1 is Loc2.
- RSU Calculates the time difference in two timestamps

  T= T2 – T1

- Now RSU calculates the distance travelled in T time by V1 using below formula.

  DISTANCE (D) = VEL * T

- RSU then calculates the approximate location of V1 at the time it sent message to V2 as follows:

  Loc = Loc1 + D

iv. RSU matches the Loc with Loc2. If it matches then it means it is benign vehicle and tells V2 to accept message.

v. If Loc doesn't match with Loc2 then it means ID is showing wrong location.

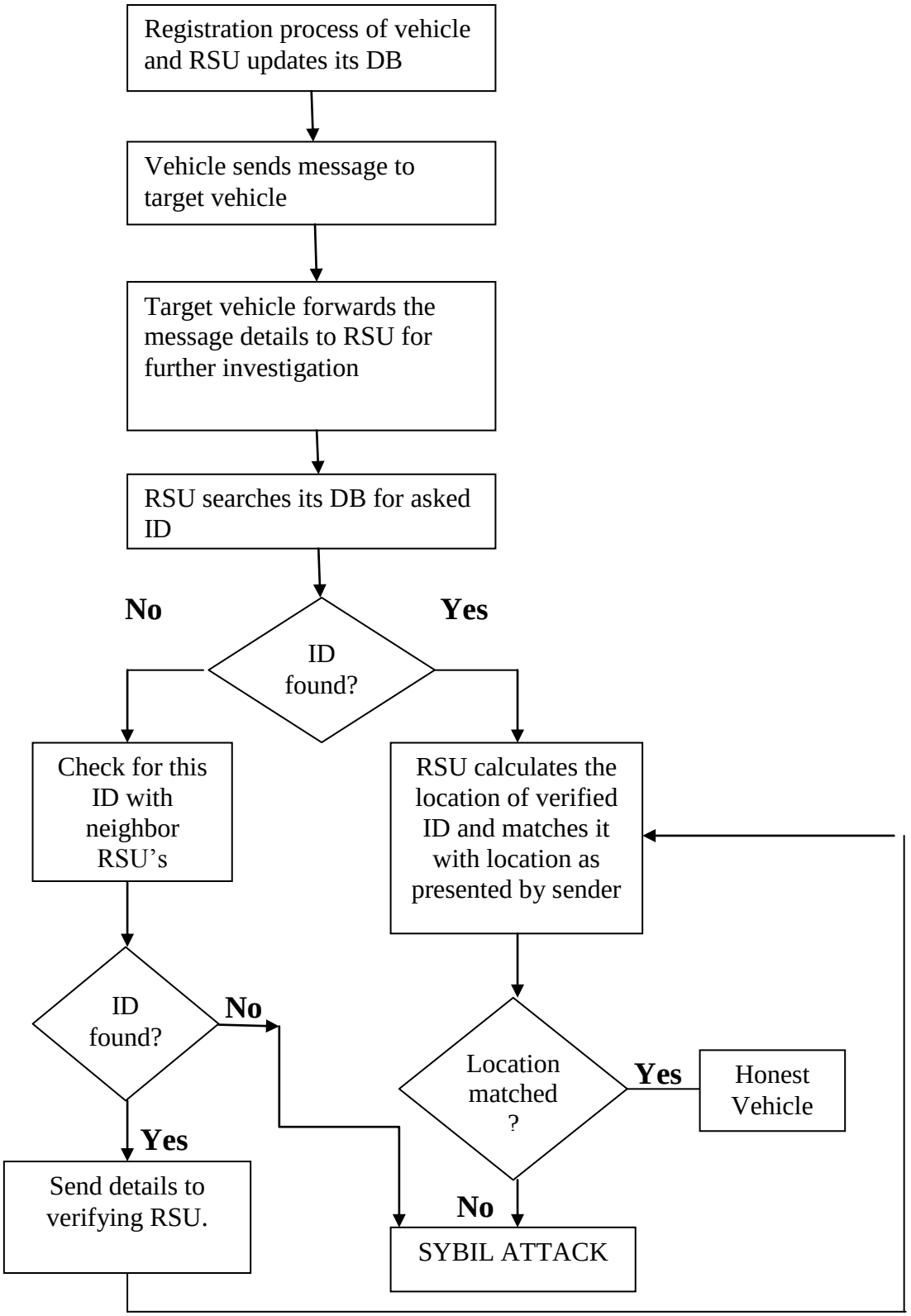
vi. Through this RSU will know that if vehicle with the particular ID is at right location as told by it. If it is not present there then it is a malicious node. RSU will revoke that particular ID and sends revoking message to the other RSU's too.

vii. If RSU is unable to find ID in its DB then it will ask its neighboring RSU's for that ID information.

viii. If ID doesn't exist at all in DB's of neighboring RSUs then it means that it is a fabricated ID.

In this way both Sybil attack scenarios will be detected.

3.4 FLOW DIAGRAM



3.5 SOFTWARE REQUIREMENT

Simulator	:	NS2 version 2.35
Language	:	TCL script
Operating System	:	Ubuntu

Chapter 4

RESULTS AND DISCUSSIONS

Figure 10 shows the first phase that is initialization phase. Vehicle is registering itself to RSU by sending registration packets as shown below.

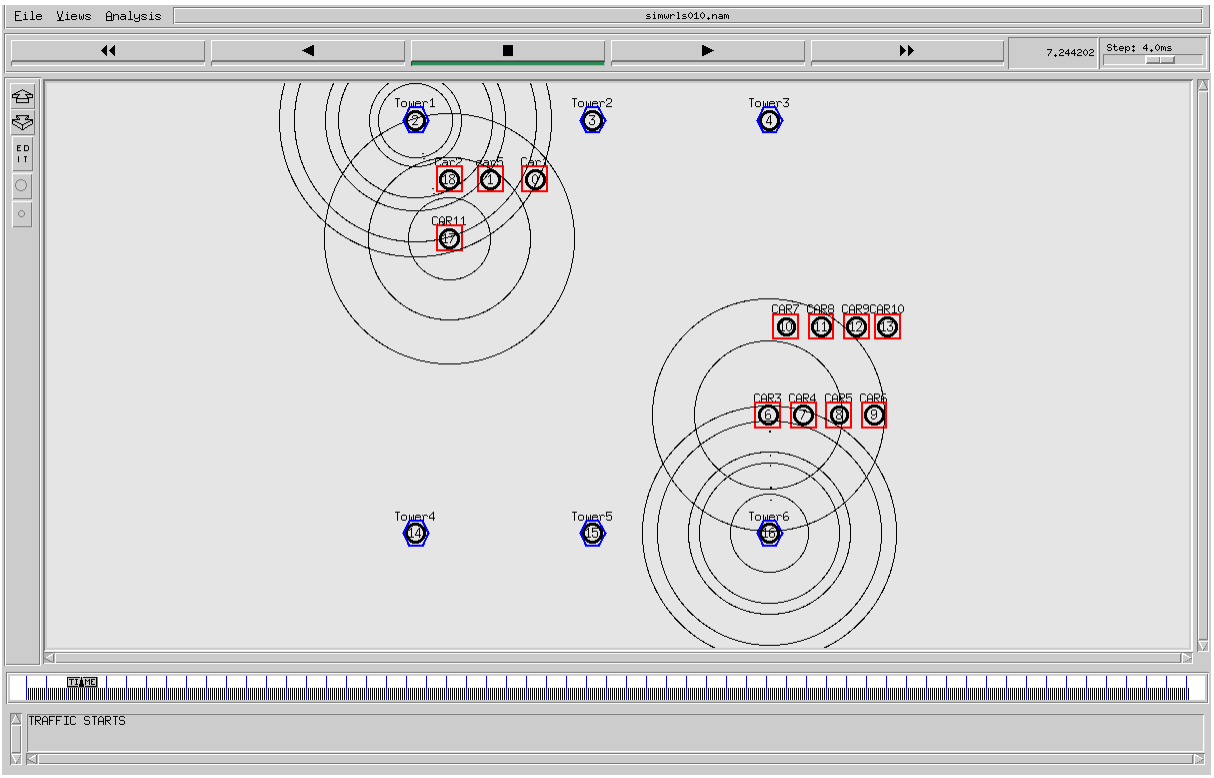


Figure 10: Vehicle registering itself

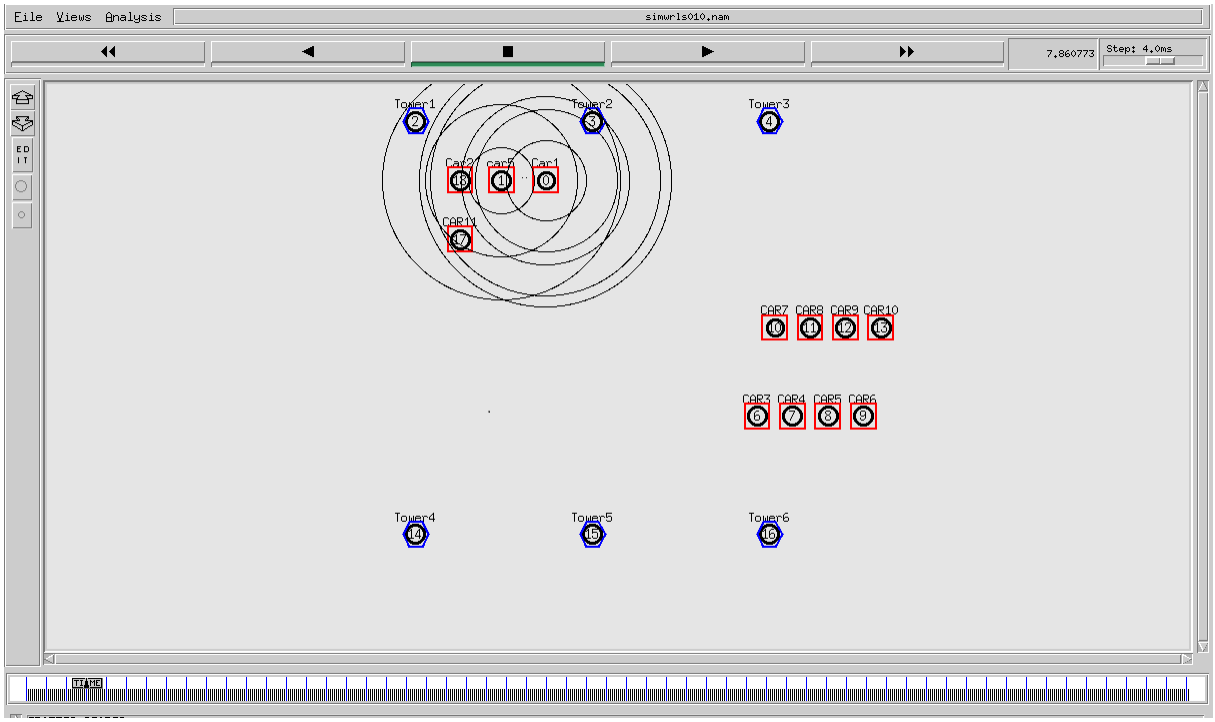


Figure 11: Inter-vehicle communication

In Figure 11, two vehicles are communicating with each other. Car 5 is sending message to Car1.

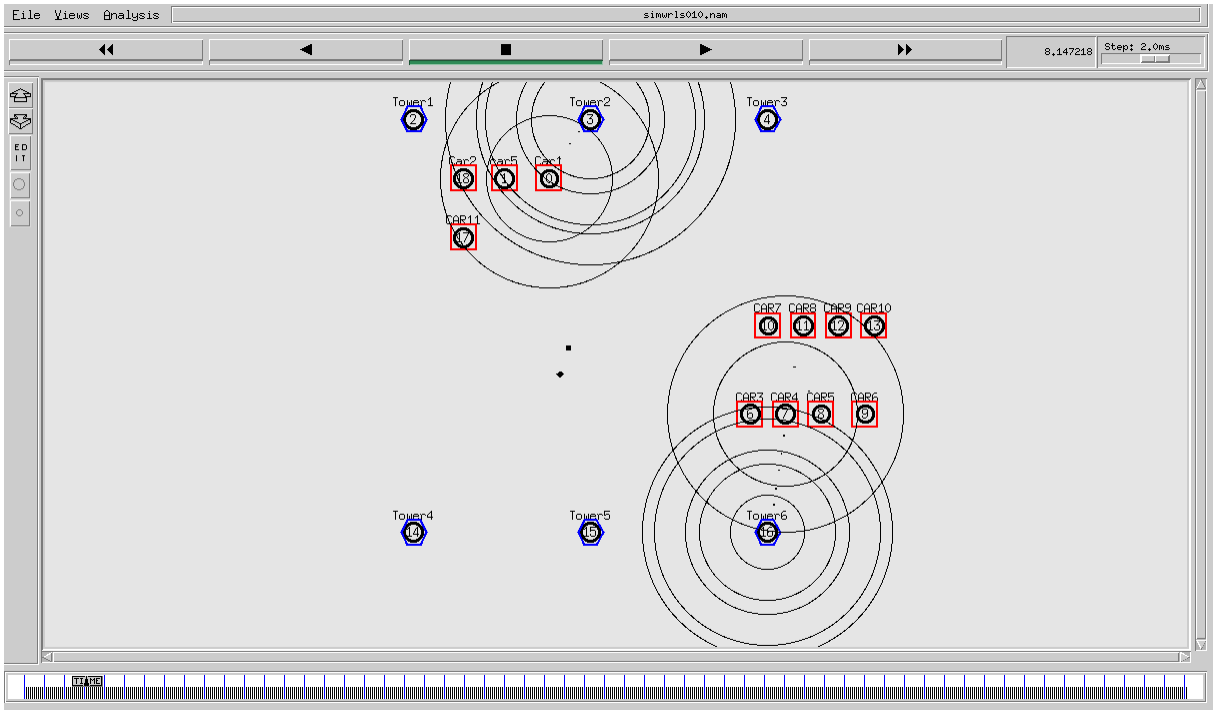


Figure 12: Confirmation of ID

In Figure 12, after receiving message from Car5, Car1 sends Car1 details to RSU to get confirmation on accepting the message or not.

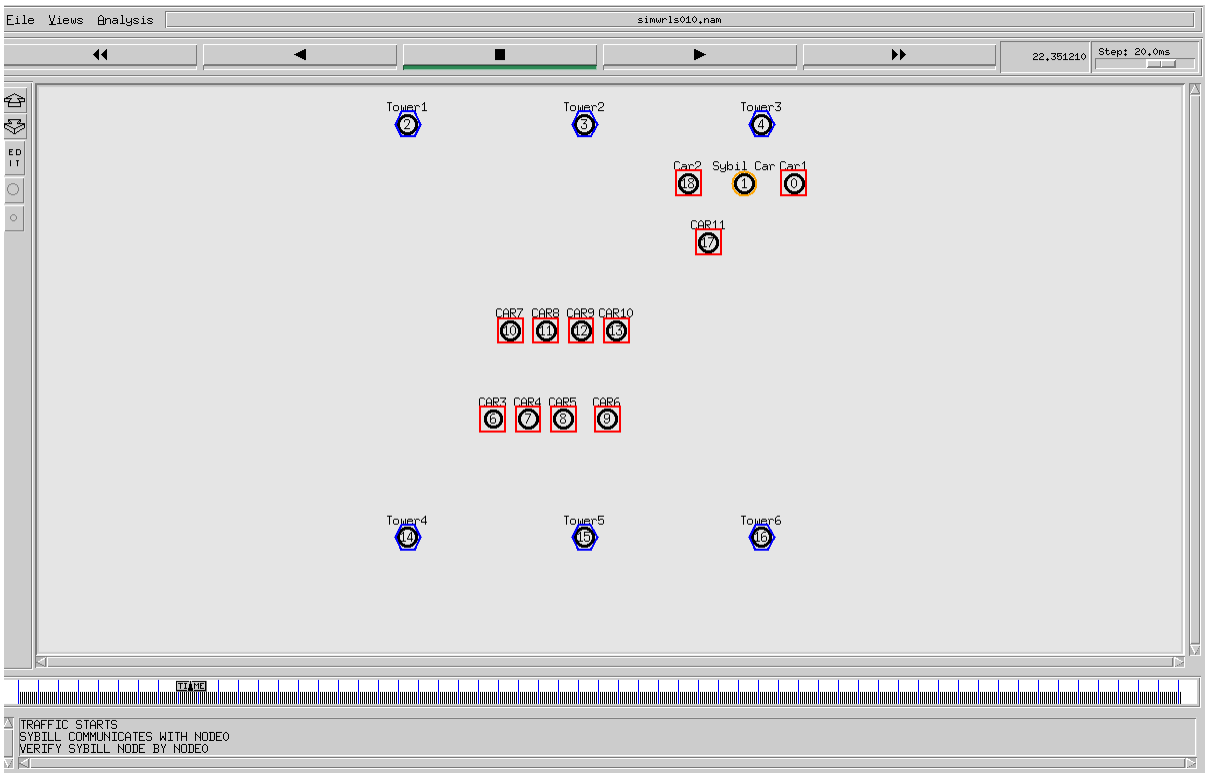


Figure 13: RSU detecting Sybil node

In Figure 13, RSU detects Car5 as Sybil node by calculating its estimated location and matching it with location shown to Car1 and hence Car5 is revoked.

Below equations are considered for evaluating simulation results-:

- Detection Rate (DR): It is defined by below given expression

$$DR = \frac{TP_d}{TP_r} * 100\%$$

  Where, TP_d is the true positive number means correct number of Sybil nodes identified by RSU. And TP_r is the number of attacks.

- False Positive Rate (FPR): It is defined by below expression where FP is number of false positives reported by RSU and NB_m is the no. of messages that are analyzed by RSU.

$$FPR = \frac{FP}{NB_m} * 100\%$$

- RSU Load: It is defined as percentage of sum of true positive plus false positive divided by number of messages analyzed by RSU (NB_m).

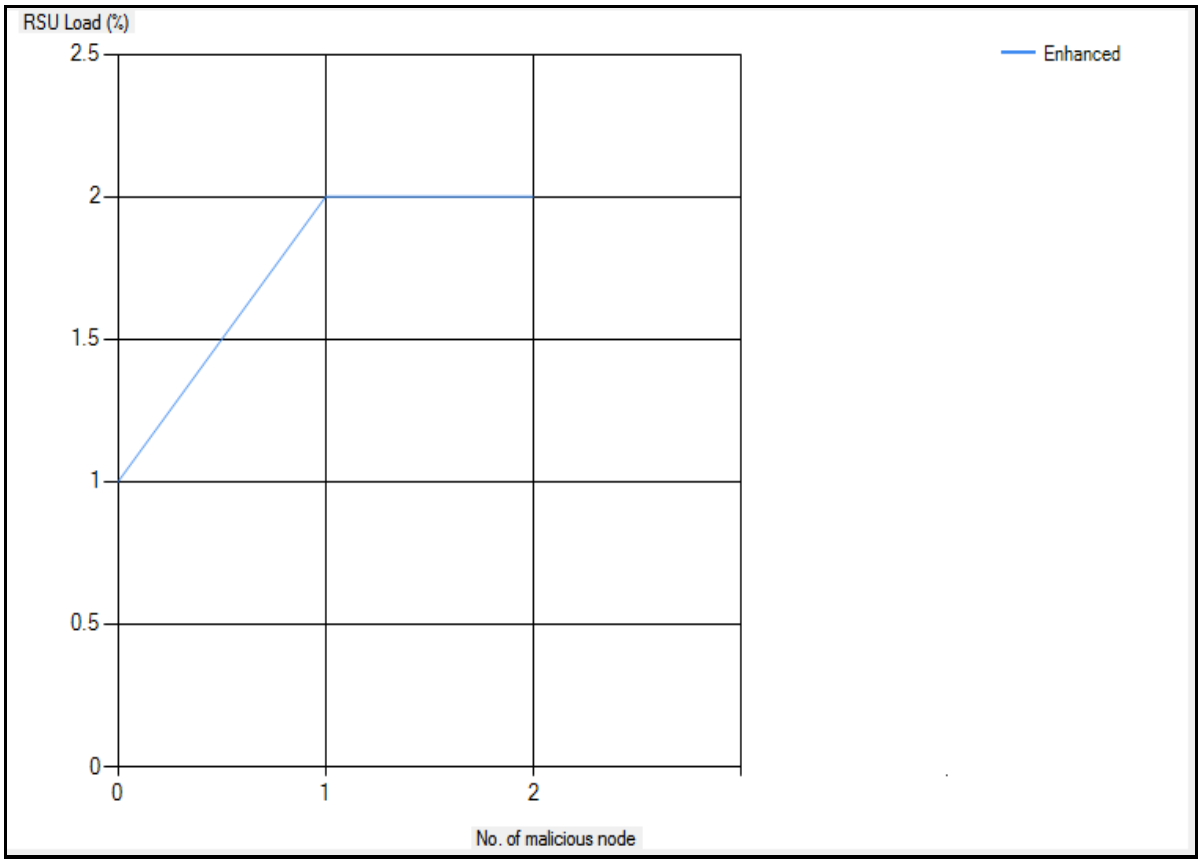


Figure 14: RSU load for 10 vehicles/km/lane

Graph in Figure 14 shows that for total number of vehicles 10, and RSU loads increases with increase in number of malicious nodes.

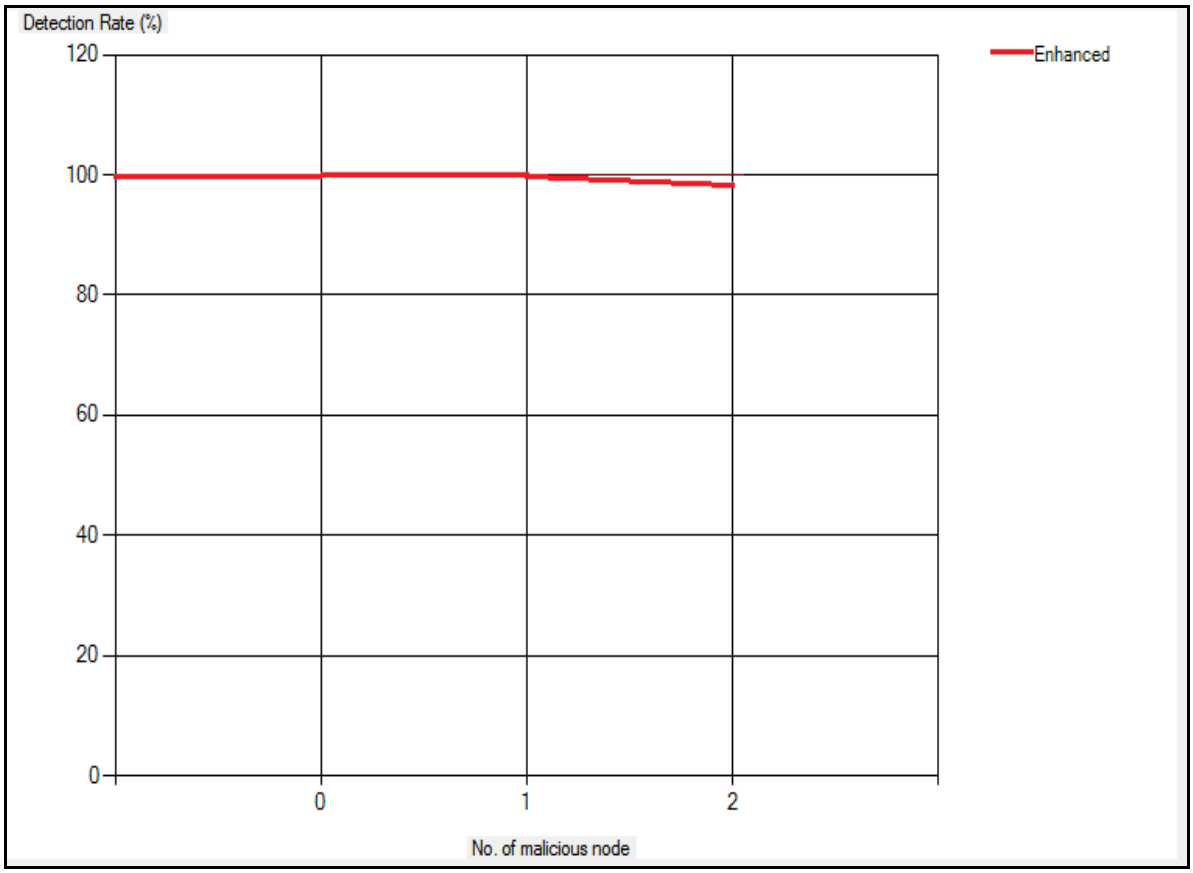


Figure15: Detection Rate for 10 vehicles/km/lane

Graph in Figure 15 shows that when number of total vehicles are 10 then detection rate of attack is 100% when number of malicious node is 0 and 1 but it decreases slightly when number increases to 2.

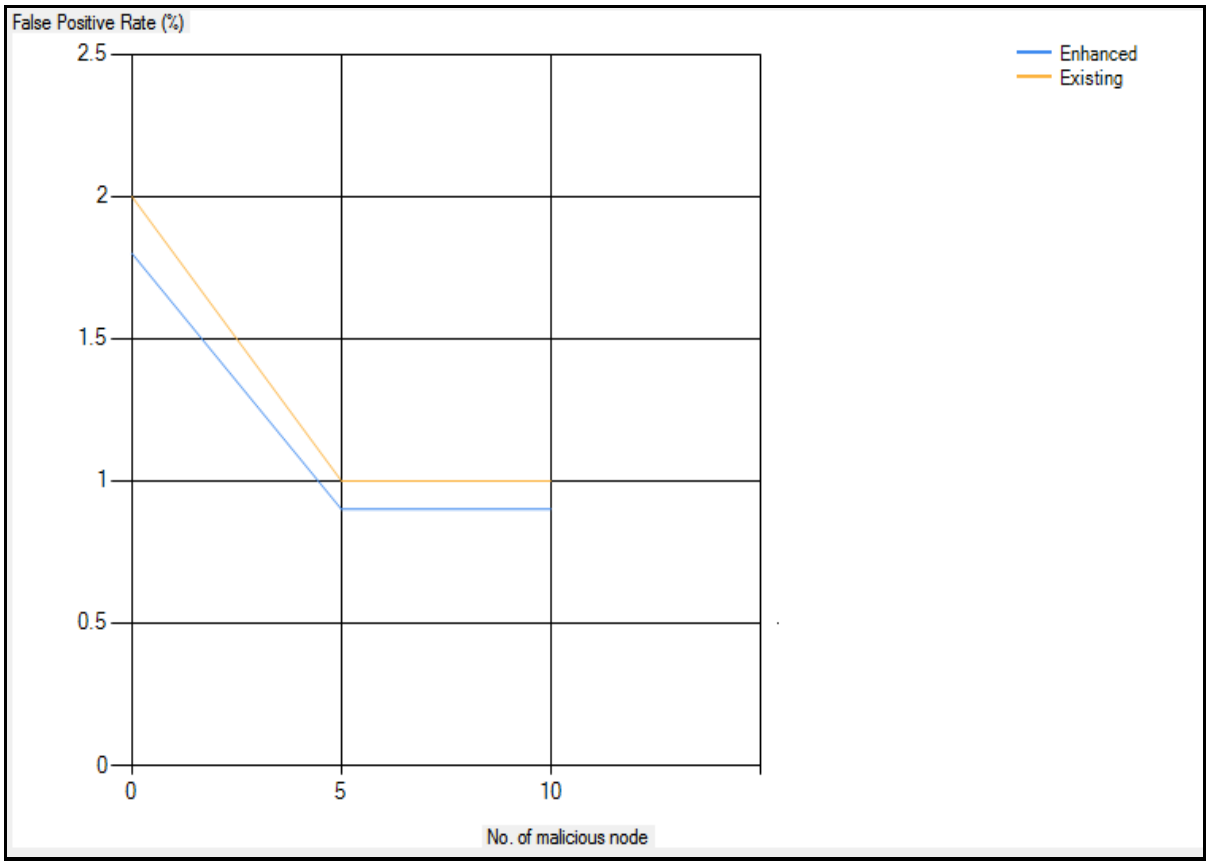


Figure16: False Positive Rate for 20 vehicles/km/lane

Graph in Figure 16 shows that when number of total vehicles are 20 then false positive rate of RSU is decreased from 2.0 to 1.8 when number of malicious node is 0 with the enhanced methodology and when number of malicious node increases, false positive rate decreases further.

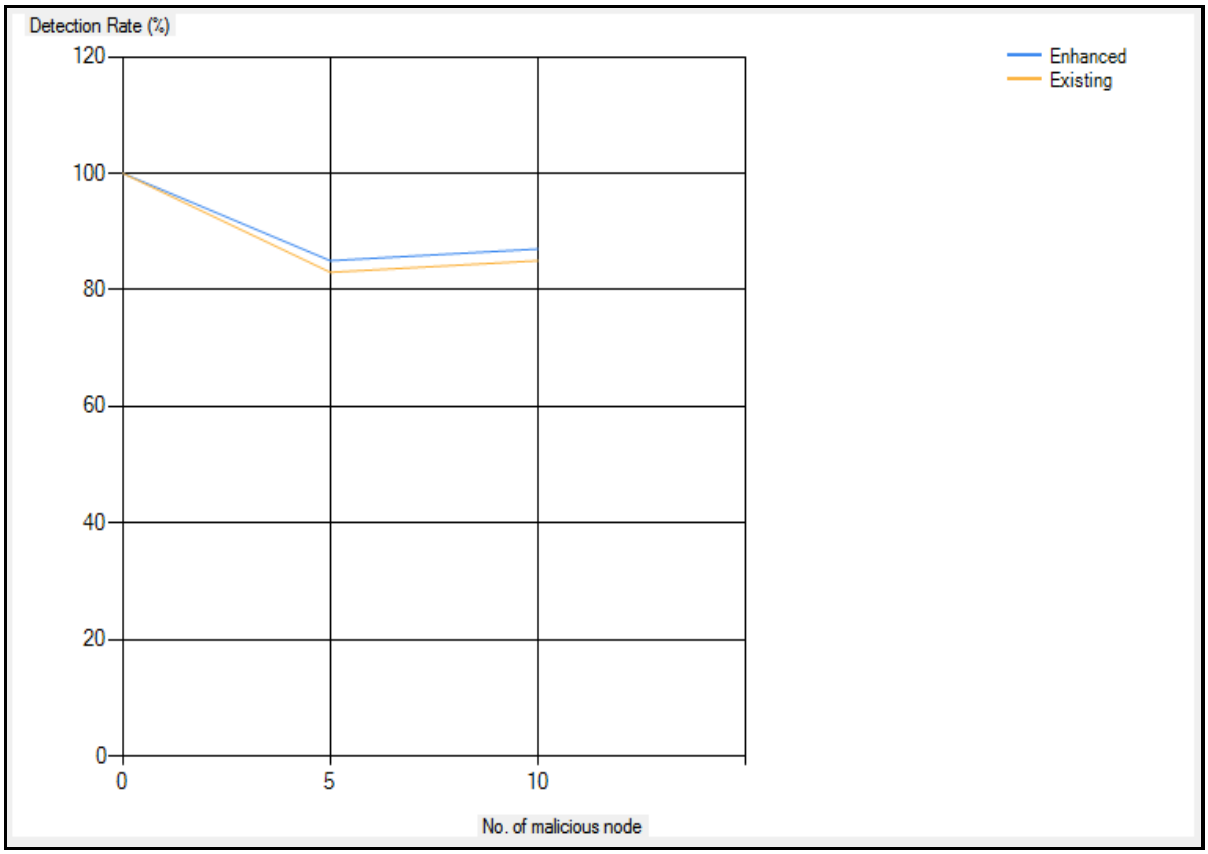


Figure17: Detection Rate for 20 vehicles/km/lane

Graph in Figure 17 shows that when number of total vehicles are 20 then detection rate is increased from 81 to 82 when number of malicious nodes are 5 with the enhanced methodology and when number of malicious node increases, detection rate increases further as compared to previous implemented mechanism.

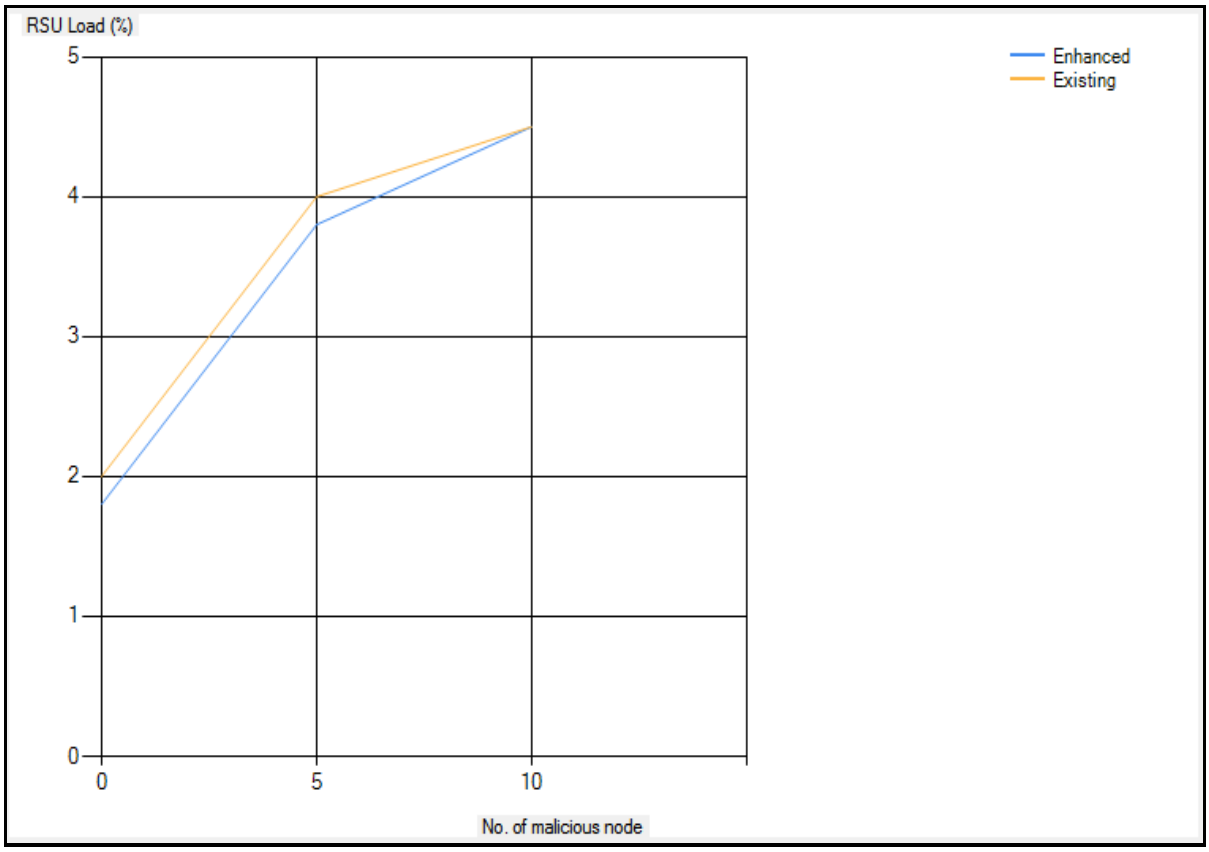


Figure18: RSU Load for 20 vehicles/km/lane

Graph in Figure 18 shows that when number of total vehicles are 20 then RSU load is decreased from 2.0 to 1.9 when number of malicious node is 0 with the enhanced methodology and when number of malicious node increases, RSU load becomes almost same as the previous implemented methodology.

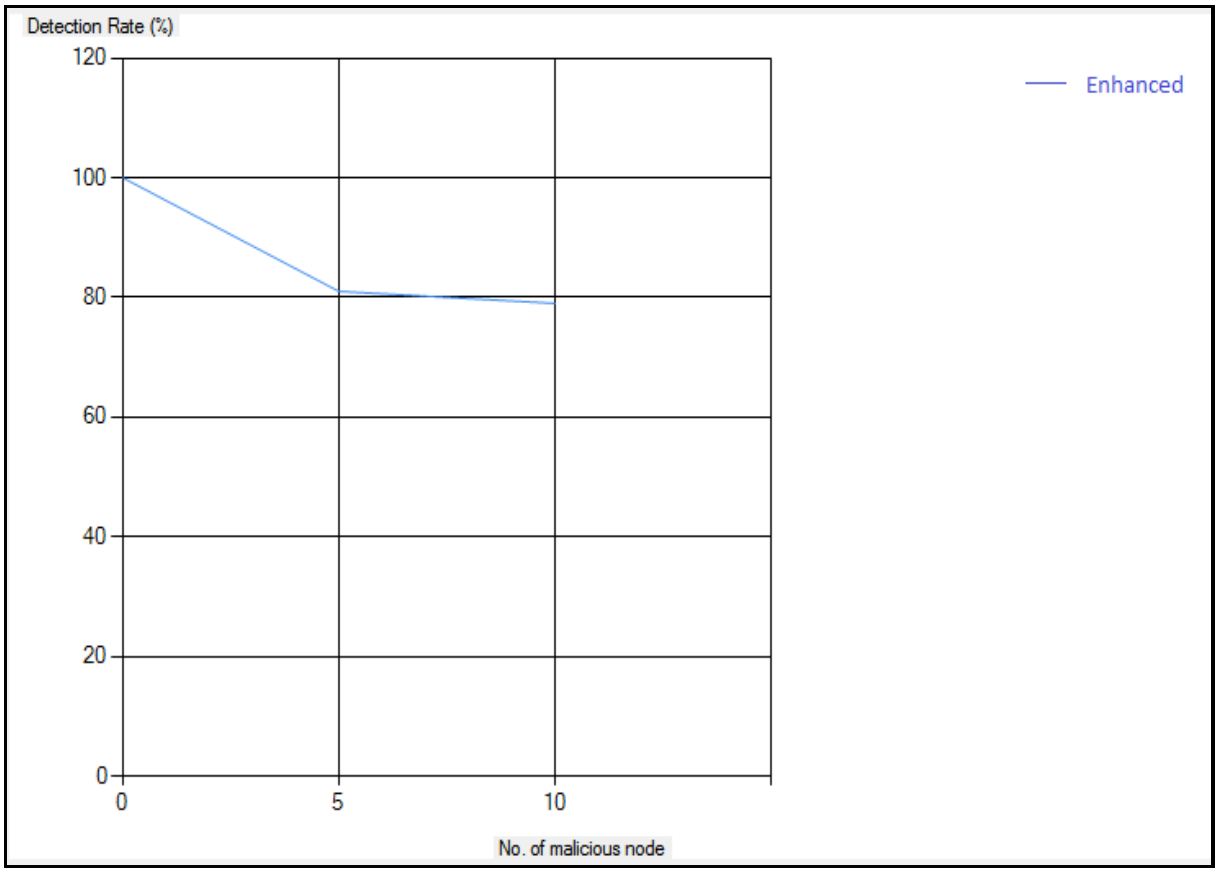


Figure 19: Detection Rate for 50 vehicles/km/lane

Graph in Figure 19 shows that when number of total vehicles are 50 then detection rate of attack is 100% when number of malicious node is 0. But it starts decreasing as the number increases.

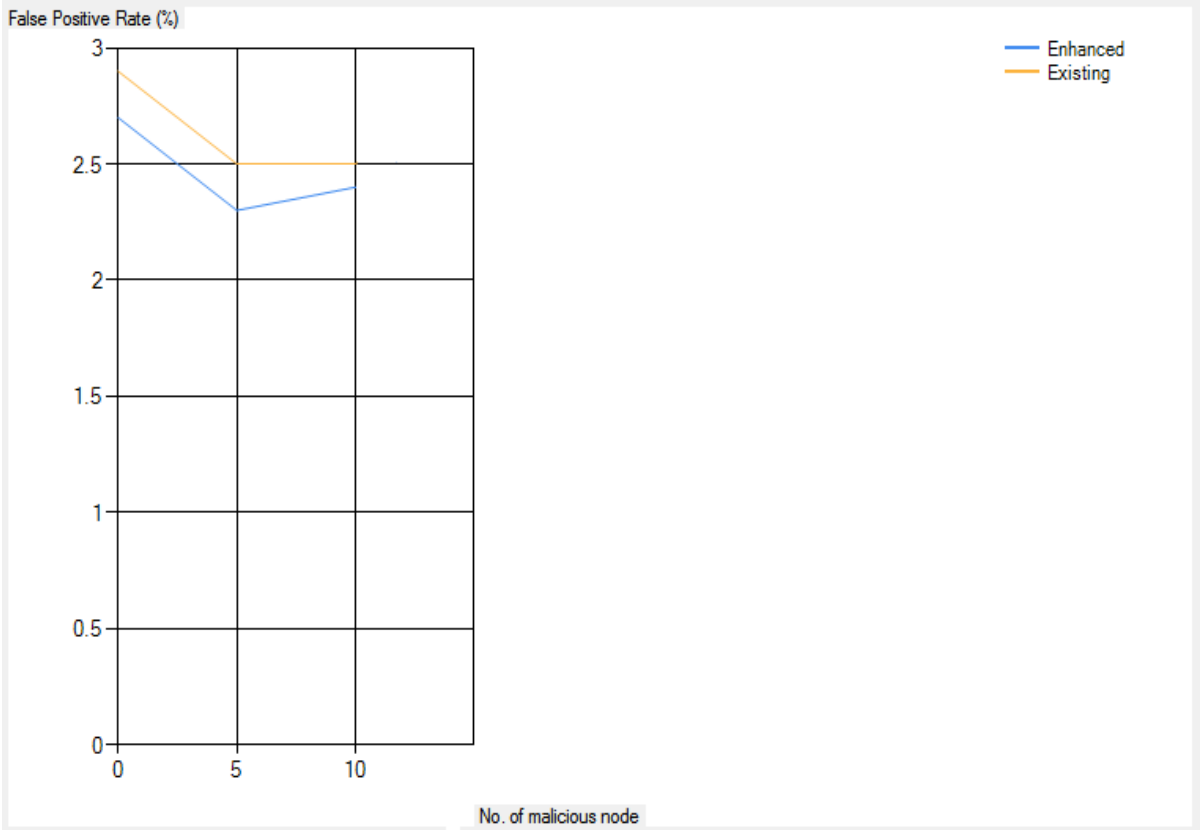


Figure 20: False Positive Rate for 50 vehicles/km/lane

Graph in Figure 20 shows that when number of total vehicles are 50 then false positive rate of RSU is decreased from 2.9 to 2.7 when number of malicious node is 0 with the enhanced methodology and when number of malicious node increases, false positive rate decreases further.

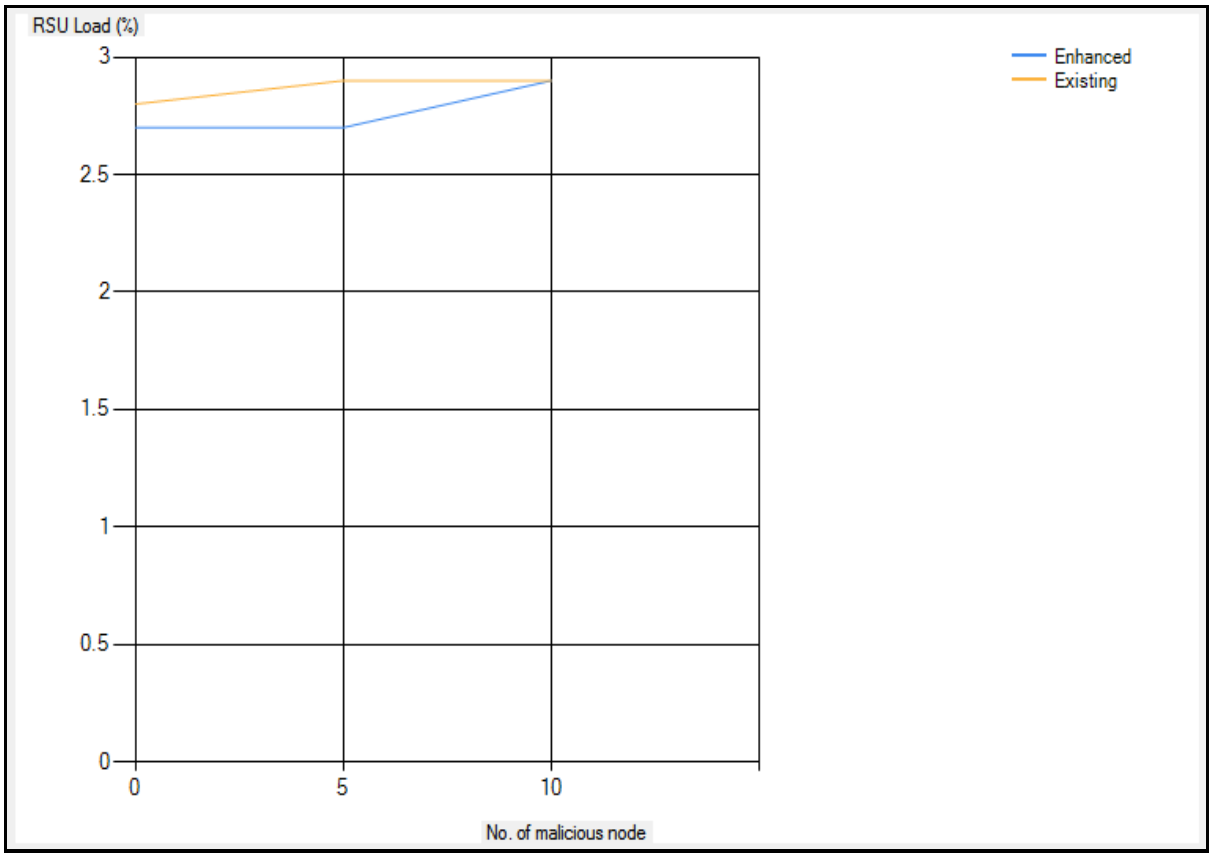


Figure 21: RSU Load for 50 vehicles/km/lane

Graph in Figure 21 shows that when number of total vehicles are 50 then RSU load is decreased from 2.8 to 2.7 when number of malicious node is 0 with the enhanced methodology and when number of malicious node increases, RSU load becomes same as is with the previous implemented methodology.

Chapter 5

CONCLUSIONS AND FUTURE SCOPE

VANET is the new upcoming technology that is being increasingly favoured for management of public areas and parking lots, accident avoidance and traffic control. So it is very important to ensure security of VANET. The detection mechanism proposed in this report works in two phases namely initialization phase and detection phase. It detects the attack with better detection rate then the existing technique. Desired results have been achieved and is proven by the resulting graphs .This mechanism detects Sybil attack at an early stage (online detection).

One of the interesting future works can be securing RSUs too which can be done based on voting mechanism by all RSUs.

Chapter 6

LIST OF REFRENCES

References from Reports

Ali Akbar Pouyan, M. A. (2014). Sybil Attack Detection in Vehicular Networks. Shahrood: Horizon Research Publishing.

Al-kahtani, M. S. (2012). Survey on Security Attacks in Vehicular Ad hoc. IEEE.

Bayrem Triki, S. r. (2013). A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks. tunisia: IEEE.

Gongjun Yan, G. C. (2007). VANET'07 Poster: Providing VANET Security Through Active Position Detection. Quebec: ACM.

J.Grover, V. M., J.Grover, V.Laxmi, M.S.Gaur (2014). Sybil Attack detection in VANET Using Neighbouring Vehicles: Geneva: Inderscience Publishers.

Jianqi Liu, J. Q. (2015). A survey on position-based routing for vehicular ad hoc networks. New York: Springer.

Kenza Mekliche, D. S. (2013). L-P2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks. Algiers: IEEE.

Kevin C. Lee, U. L. (Oct 2009). Survey of Routing Protocols in Vehicular Ad hoc Networks. In "Survey of Routing Protocols in Vehicular Ad Hoc Networks," Kevin C. Lee, Uichin Advances in Vehicular Ad-Hoc Networks: Developments and Challenges.

Maxim Raya, J.-P. H. (2007). Securing Vehicular Ad Hoc Networks. Journal of Computer Security .

Mina Rahbari, M. A. (2011). Efficient Detection of Sybil Attack Based on Cryptography in VANET. International Journal of Network Security & Its Applications (IJNSA).

Mohamed Salah Bouassida, G. G. (2008). Sybil Node Detection Based on Received Signal Strength Variations Within VANET. France: Academia.

Mostofa Kamal Nasir, A. D. (2013). Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH.

Mukul Saini, K. K. (Nov 2013). Efficient and Feasible Methods to Detect Sybil Attack in VANET. International Journal of Engineering Research and Technology , 431-440.

Nicole El Zoghby, V. C. (2012). Distributed Data Fusion for Detecting Sybil Attacks in VANETs. Springer.

P.Vinoth Kumar, M. (2014). Prevention of Sybil Attack and Priority Batch Verification in VANETs. Tamil Nadu: ICICES.

Parastoo Kafil, M. F. (2012). Modeling Sybil Attacker Behavior in VANETs. Tehran: IEEE.

Parastoo Kafil, M. F. (2012). Modeling Sybil Attacker behavious in VANETS. Tehran: IEEE.

Rasheed Hussain, S. K. (2012). Privacy-Aware VANET Security: Putting Data-Centric Misbehavior and Sybil Attack detection Schemes into Practice . Korea.

Shan Chang, Y. Q. (2012). Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. IEEE Computer Society.

Soyoung Park, B. A. (2011). Defense Against Sybil Attack in Vehicular Ad Hoc Network. Orlando: Computer Science at UCF.

Thiago M. de SALES, H. O. (2014). A Privacy-Preserving Authentication and Sybil Detection. C.A: IEEE.

Tong Zhou, R. R. (March 2011). P2DAP – Sybil Attacks Detection in Vehicular. IEEE.

Yong Hao, J. T. (2011). Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs. Chicago: IEEE.

References from Website

Mahmoud Al-Qutayri, C. Y.-H. (2010). Security and Privacy of Intelligent VANETs. Retrieved from www.intechopen.com: http://www.intechopen.com/books/computational-intelligence-and-modern-heuristics/securityandprivacyofintelligentvanets